Omnissa 보안 액세스를 통한 전체 클라이언트 연결 문제

목차

문제

Omnissa 전체 클라이언트가 Cisco Secure Access를 통해 연결된 경우 가상 데스크톱을 로드할 수 없습니다. 사용자는 전체 클라이언트 애플리케이션을 사용하여 가상 환경에 연결을 설정하려고 시도할 때 연결 실패를 경험합니다. 그러나 HTML/웹 클라이언트를 통한 액세스는 계속 정상적으로 작동하므로, 기본 가상 데스크톱 인프라가 작동하지만 Cisco Secure Access 솔루션을 통해 연결을 설정하는 클라이언트의 전체 기능에 영향을 주는 특정 문제가 있음을 나타냅니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: Cisco 보안 액세스
- 제품군: 초
- 소프트웨어 버전: 영향을 받는 모든 버전
- 클라이언트 애플리케이션: Omnissa 전체 클라이언트
- 가상 데스크톱 환경: Omnissa 가상 데스크톱
- 네트워크 인프라: IPsec 터널 및 FTD(Firepower 위협 방어)

해결

해결 방법에는 Cisco Secure Access를 통해 Omnissa 전체 클라이언트에 대한 적절한 라우팅을 활성화하기 위한 특정 네트워크 컨피그레이션 변경을 구현하는 것이 포함됩니다. 연결 문제를 해결하

기 위해 다음 단계를 수행했습니다.

- 스플릿 터널 설정을 구성합니다. Omnissa 전체 클라이언트가 필요한 대상 호스트에 대한 직접 연결을 설정할 수 있도록 스플릿 터널 구성을 추가합니다. 이 컨피그레이션을 통해 특정 가상 데스크톱 클라이언트로 향하는 트래픽이 적절한 네트워크 경로를 통해 올바르게 라우팅되도록 합니다.
- 고정 경로 컨피그레이션을 구현합니다. 가상 데스크톱에 대한 연결을 설정해야 하는 특정 클라이언트에 대한 고정 경로를 구성합니다. 핵심 요구 사항은 어그리게이션 서버 다운스트림뿐 아니라 가상 데스크톱 클라이언트가 연결해야 하는 대상 호스트로 직접 경로를 구성하는 것입니다.
- IPsec 터널 지우기 컨피그레이션 변경 사항을 구현한 후 FTD에서 IPsec 터널을 지워 새 라우팅 컨피그레이션이 제대로 적용되는지 확인합니다.
- 연결을 확인합니다. 변경 사항을 구현한 후 Omnissa 전체 클라이언트 연결을 테스트하여 Cisco Secure Access를 통해 가상 데스크톱 연결을 성공적으로 설정할 수 있는지 확인합니다 .

구현 일정

사용자에게 미치는 영향을 최소화하려면 예약된 유지 관리 기간 동안 컨피그레이션 변경을 구현해야 합니다. 구현 후 Omnissa의 전체 클라이언트 연결과 연결성을 모두 검증하여 성공적으로 해결되었는지 확인합니다.

원인

연결 문제는 Cisco Secure Access 환경의 라우팅 컨피그레이션이 충분하지 않아서 발생했습니다. 특히, 네트워크는 어그리게이션 서버 다운스트림에 대한 경로로만 구성되었지만 Omnissa 전체 클라이언트가 연결을 설정하는 데 필요한 특정 클라이언트에 대해 필요한 스플릿 터널 및 고정 경로 컨피그레이션이 없었습니다. 이러한 라우팅 격차로 인해 전체 클라이언트가 가상 데스크톱 호스트에 제대로 도달할 수 없었지만, HTML/웹 클라이언트는 적절하게 구성된 서로 다른 연결 경로를 사용하므로 계속 작동할 수 있습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.